Amendments to the Specification:

Please replace the paragraph beginning at page 1, line 12, with the following rewritten paragraph:

a1

Flooding attacks have recently been used with increasing frequency to target and disable servers on the Internet. A flooding attack occurs when a user sends a large number of requests to a server in a relatively short period of time with an intent to overload and thereby disable the server. A flood of packets from a malicious user can overload a server in the same way that a flood of packets from a misconfigured system can overload a server. But the end result is the same; the server becomes overloaded in trying to service the requests. This prevents legitimate requests from being timely served and often disables a server or causes it to crash. A number of flooding attacks have been reported in the news recently on some well known web sites. These attacks were characterized by a flood of individual connection requests to establish initial communications. A related patent application, serial number [[   ]]09/502,478 filed February 11, 2000, discloses an algorithm to defend against such connection request attacks. However, it is also possible to attack a server by flooding it with connectionless datagrams, such as might occur in the UDP (user datagram) protocol. The effect is essentially the same; the server becomes overloaded in trying to service the horde of datagrams and can even become totally disabled. Flooding attacks are very difficult for traditional intrusion detection systems to prevent due to the difficulty of determining whether the traffic is legitimate or not.